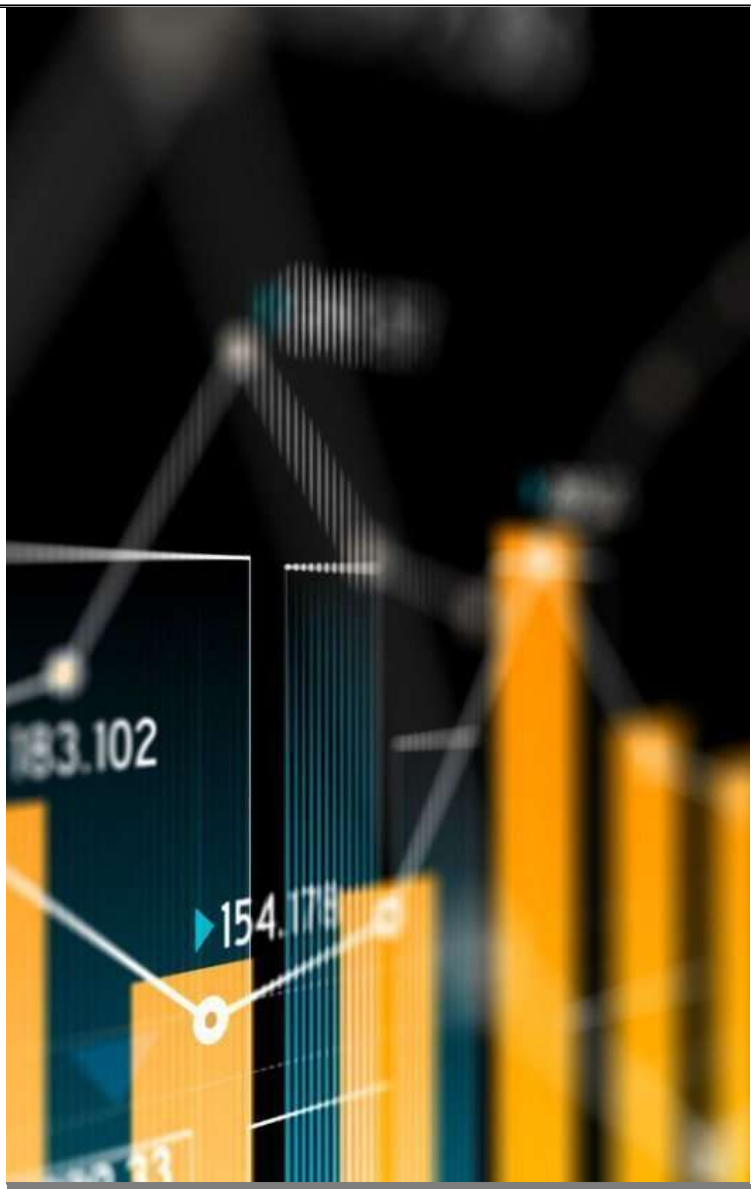
FRAUD TRENDS GLOBALLY AND IN SOUTH AFRICA



CELEBRATING 10 YEARS OF EXCELLENT SERVICE

RMG FORENSIC SERVICES (Pty) Ltd.

DECEMBER 2020

Version 1

marketing@rmgforensics.com

www.rmgforensics.com

RMG Forensic Services is proud to employ Certified Fraud Examiners

Index

Subject for this fraud newsletter version 1/2020:

ACCOUNTING FRAUD IN YOUR ORGINIZATION

Foreword

As part of the Fraud Awareness initiative of the MRG Group to its members this monthly Fraud newsletter would assist with the most current Fraud Trends detected in the industry as well as practical advice to proactively remedy this.

In this month's fraud newsletter version 1/ 2020 we cover the subject at hand: *on the book fraud* which is also known as *accounting fraud*. We will explain the definition and this *modes operandi of the fraud* and provide tips on how to prevent it.

In the next edition newsletter version 2 / 2021 in the first quarter of the year we will define cyber security threats in the South African and in the global context.

Accounting Fraud – On the Book Fraud

On the Book Fraud – this is when an employee or someone else in a trusted position steals from your business. They use the money or other assets for their own use.

On the Book Fraud Examples

Here are the top 25 on the book fraud examples and workplace thefts to watch out for:

- Forging Checks
- Cashing Customer Checks
- Faking Vendor Payments
- Overbilling Customers
- Theft of Customer Card Data
- Padding an Expense Account
- Double Dipping
- Using a Company Credit Card for Personal Use
- Voiding Transactions at The Cash Register
- Siphoning Off Cash Deposits
- Raiding the Petty Cash Box or Safe
- Pocketing Cash from Fundraisers
- Stealing Office Supplies
- Stealing Equipment or Raw Materials
- Stealing Products
- Burglarizing Company Premises
- Stealing Returned Merchandise
- Claiming a Company Laptop Was Lost
- Setting Up Fake Employees
- Falsifying Overtime
- Failing to Remit Payroll Tax Money
- Collecting Kickbacks from Vendors
- Selling Trade Secrets; Corporate Espionage
- Business Identity Theft
- Starting A Business Using Company Resources

Business Fraud in South Africa

Business fraud is the crime that is least talked about because it is not as headline grabbing as armed robberies, and more importantly many businesses do not report this type of crime because they are afraid of reputational damage should it become public knowledge.

Fraud cost the African continent $8.9 billion in the second half of 2018, with three-quarters of all fraud cases reported in Nigeria, Kenya, Zimbabwe, Tanzania, and South Africa, According to the latest African Fraud Barometer. One can only imagine that it had quadrupled by 2020.

In its Global Economic Crime Survey 2018 auditing firm PwC revealed that in comparison to businesses globally, South African businesses experienced more fraud and bribery incidents than their counterparts globally. The survey went on to say that South African organizations reported that senior and middle management commit 77% of all internal fraud and that the profile of the typical fraudster is:

- Male
- Aged between 31 and 40,
- Has worked for his employer for more than 10 years
- Has acquired a university degree

There six common financial frauds that can affect a company and if not caught or stopped before they happen can financially ruin a company. Too often we hear of business owners that have found out too late that a “long time trusted” employee is suspected of stealing from the company. Most corrupt offenders are only identified after the employee has been appointed to the job, by means of a pre-employment screening investigation possible fraud could be mitigated.

The six-basic type of financial business fraud are:

- **ON THE BOOK FRAUD** – fraud or misappropriation of funds placed in one's trust or belonging to one's employer. A bookkeeper or other employee may have come into hard times financially and has resorted to using his/her employers funds for personal expenses.

- **EMPLOYEE FRAUD** – is defined as any stealing, use or misuse of an employer's assets without permission. The term employer's assets are important because it implies that employee theft involves more than just cash. This type of theft is sometimes referred to “inventory shrinkage”.

- **PAYOFFS & KICKBACKS** – this is where employees accept cash or other benefits in exchange for access to the company’s business defined as corruption.

- **SKIMMING** – this occurs when employees take money from receipts and do not record the revenue on the books.

- **DOUBLE PAYMENT FRAUD** – a bookkeeper would typically pay an invoice twice when paying an invoice.

- **CYBER-CRIME** – These can include “phishing attacks”, EFT payment fraud, identity theft, bank account fraud, ransomware, CEO fraud, hack attack, denial of service attacks to name a few.

It is vital to an organization, large or small, to have a **fraud prevention strategy** in place. On average fraudulent activities can last an average of 18 months before being detected.

There are steps you can take to reduce the risk of your company becoming a fraud statistic.

- **Know your employees before you hire them** – Conduct a thorough pre-employment screening check on them. These checks can weed out those with prior convictions for financial crimes, confirm references with prior employers ensuring the company information given is not a friend on the other side of the line giving a glowing reference, check that qualifications claimed are indeed factual and much more.

- **Employees awareness** – Everyone within the organization should be aware of the fraud risk policy including types of fraud and the consequences associated with them.

- **Implement internal controls** – Segregation of duties is an important component of internal control that can reduce the risk of fraud from occurring, checks and balances, known as “red flags”.

- **Mandatory vacations** – You might be impressed by the employees who haven’t missed a day of work in years. While you may think that these loyal hard-working employees, it could be a sign that these employees have something to hide and are concerned that someone will detect their fraud if they were out of the office for a period of time. Many bookkeepers were caught only when they were forced to take a vacation and a temp was in doing their job.

- **Hire experts** – If you suspect that there is possible fraudulent activity going on in your company or the recent break-in just does not make sense as no one can figure out how they got in, call an expert. Even if nothing is found it will give you peace of mind.

“Business fraud is a big problem and we have seen an increase in this type of case coming into our office not only here but in the rest of the country, so it is a global issue. Most clients come to us because they do not want it getting out and becoming public for obvious reasons. We have seen it all; cyber-crime, employee theft, employees that team up with outsiders to break into offices and much, much more. Business owners must be more vigilant as to who they hire when we perform pre-employment screening checks for clients, we have noticed an increase of applicants with serious criminal convictions and more and more false qualifications, some of the job applicants we investigate have as many as 20 criminal convictions. The slogan should be ‘CHECK BEFORE YOU HIRE’ it will save you future problems”

TYPES OF CORRUPTION	2017	2018	2019
BRIBERY	29.5%	23%	34%
IRREGULARITIES IN PROCUREMENT	12.7%	16.9%	41%
THEFT OF RESOURCES	14.4%	11.3%	28%

5 Tips to Avoid Employee on the Book Fraud

Employee theft and On the Book, Fraud can happen in any business. However, it hits smaller businesses in larger numbers, in part because too often owners do not have the right checks and balances in place.

The following are five tips that can help you greatly reduce the chance that you are victimized.

If we have heard it once, we have heard it a thousand times: “I trust my bookkeeper.” Almost every case of On the Book Fraud in small businesses involves a person who is trusted, taking money from an unsuspecting business owner.

We have seen a lifelong best friend steal from her business partner. We have seen a man take money from his siblings.

Honest, hardworking entrepreneurs have been taken for tens and hundreds of thousands of Rands. The owner’s mistake: they trusted too much. When you think it cannot happen to you, your business is the most susceptible.

Trust, but verify
- Ronald Regan

Many business owners do not want to put financial controls in place because they are afraid of making their bookkeeper feel distrusted. That logic is flawed. An honest bookkeeper would want checks and balances so that there could never be a question about his or her veracity. In fact, the bookkeepers we have seen complain the most about not being trusted are the ones who were later found to have been stealing from the company.

Further, it is fundamentally unfair to your bookkeeper to give him or her unfettered access. At some point he or she is going to face financial difficulties -- almost all of us do. Why tempt a person when he or she is most vulnerable by giving him or her uncontrolled access to your cheque book?

1. Run all receipts and disbursements through a checking account.

Put any money that comes into the business into a checking account. Take any money that leaves the businesses out of a checking account. This provides a record of receipts and disbursements that cannot be tampered with because it's controlled by the bank.

Bookkeepers can put false entries into financial statements, but they can't manipulate cash in the bank. Everything should be reconciled to the checking account. The reconciliation should happen monthly, and the owner should review it in a timely manner. It only takes a few minutes.

2. Create Segregation of Duties.

We advise that the same employee not set up a vendor, approve a payment and write the check. It is better to have two people involved when money leaves the business. In the same way, one employee should not set up an employee on the payroll system and cause a paycheck to be cut. One bookkeeper, who is now living at the expense of government, set up a fake employee to funnel money into her own account.

3. Review statements.

The owner should periodically and unpredictably review bank statements, credit card statements and statements from the payroll company showing what each employee was paid. This should include looking at cancelled checks. After years of blind trust, one business owner finally reviewed a bank statement and found that her trusted bookkeeper was making cash withdrawals from ATMs, writing checks to himself and using his company debit card to purchase personal items such as groceries.

4. Mandatory Audits:

Periodically, have an unrelated third party review your books and accounts. This does not have to be a comprehensive audit of every transaction -- spot checks will do. The cost is minimal, and the deterrent can save you thousands.
Employee theft and fraud is a massive problem. Statistics reveal that it results in one-third of all small-business failures. Set up the simple financial controls necessary to prevent it. Do not let your business become yet another statistic.

Don't

- Give end-to-end responsibilities for accounting – segregate duties
- Send bank financial statements directly to the accounting department. Have someone outside the department to review them first
- Assume long term employees are incapable of fraud and corruption
- Stop at a criminal and credit checks for employees who will be handling money. Continue to run background checks even after the hire date
- Allow fraudsters to leave your employment without pursuing a conviction.

Do

- Implement checks and balances
- Send bank statements to business owners' home
- Pay attention to employee lifestyles and extreme changes to them
- Promote a culture of trustworthiness and integrity
- Talk with all employees about fraud detection and internal controls. Have them sign a code of ethics.
- Complete background and credit checks and criminal checks on employees who will be handling money

Trends Reported by the Industry

According to SAICB, the economic desperation caused by COVID has led to an increase in the following opportunistic crimes:

- **FAST TRACK CLAIMS ON:**
  - Phones, Tablets & Laptops…
  - Keys, Glasses etc.…
- Fake Retrenchments and UIF Fraud.
- Credit Life submissions.
- Credit Insurance Losses.
- Staged “Slip & Trip” type incidents.
- Creation of Fake Disabilities.

- **IMPERSONATION OF:**
  - Corporates – through websites, links, and call centers.
  - ID theft of Individuals.
  - Fake Charities.
- Increase in false Death Claims.
- Upsurge in Economically driven Physical Crimes, Hijacking, Thefts and even Murder.
- Cyber Incidents - Mail Interception, Phishing, Vishing, and targeted cyber

“Looking at the broader environment in which we all live and work, it is obvious that both organizations and individuals have dramatically altered the way they think and operate in order to survive the effect of COVID.” - **SAICB**

The following is an excerpt from the 2019 annual crime stats report from SABRIC (The South African Banking Risk Information Centre)

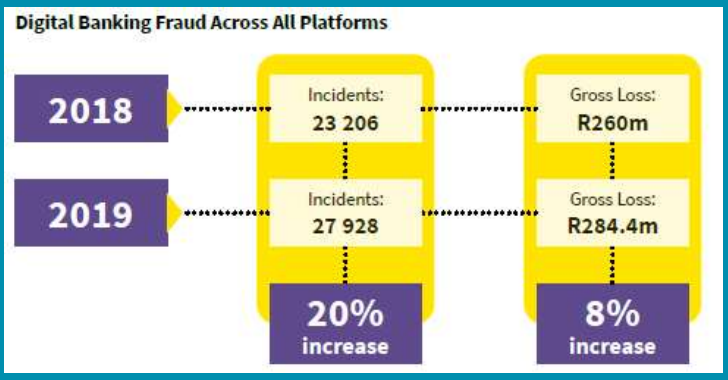
Financial crime is largely influenced by contextual events. The global technical recession has seen South Africa's economy shrink providing criminals with the impetus as well as opportunity to commit financial crimes.

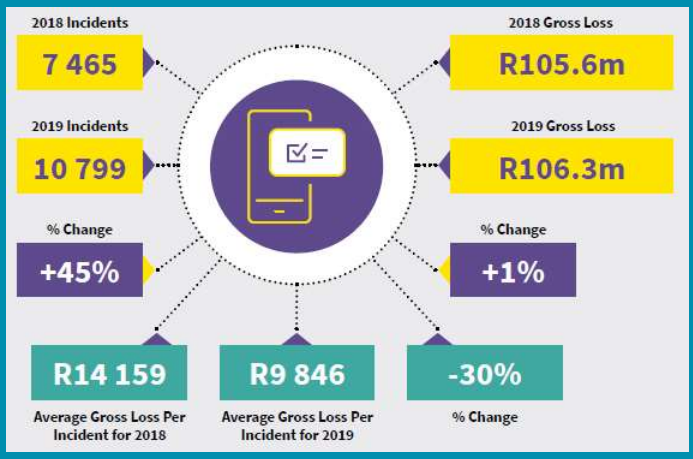
During 2019, the banking industry experienced increases in burglary and robbery incidents. However, it is evident that putting the correct collaborative structures in place is the key to mitigating these crimes which has seen these incidents decline by 16%.

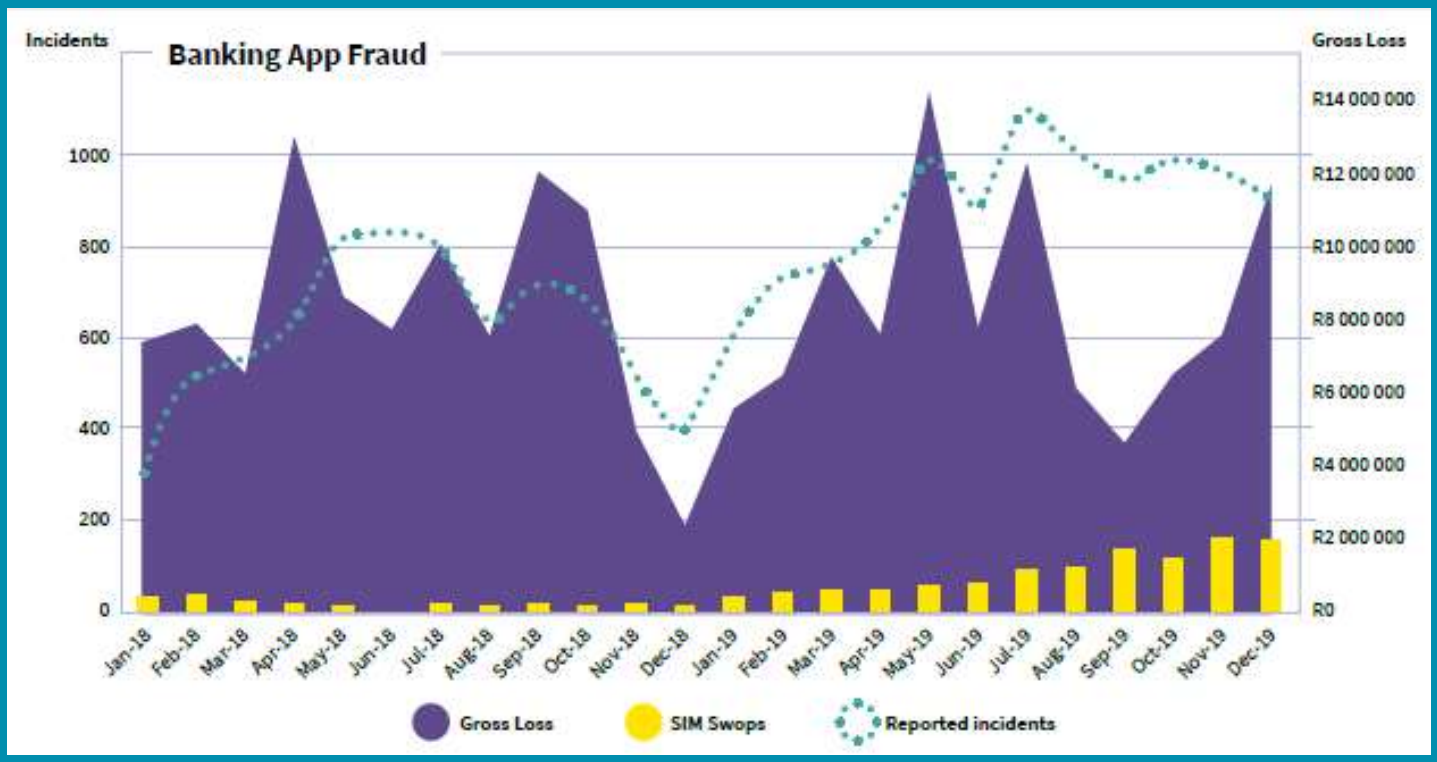
Although syndicates continue to orchestrate crimes involving the theft/robbery of physical cash, the evolution of the digital landscape has seen the emergence of cybercrime which is increasing at an alarming rate. These crimes will eventually replace many 'traditional' banks crimes as they transcend time and physical proximity due to their virtual nature. Digital banking incidents increased by 20% in 2019, a number that is set to rise in the future, as criminals continue to use social engineering tactics to extract personal and confidential information from victims, enabling them to transact on their accounts without authority.

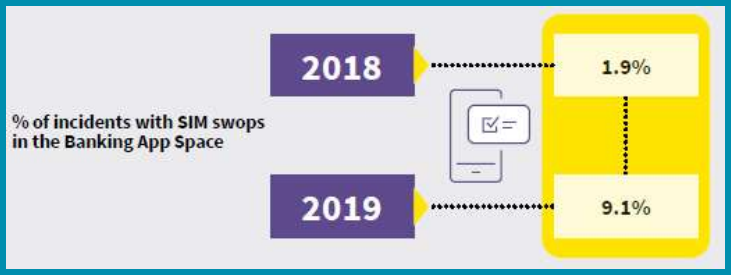
As with cybercrime, gross fraud losses on South African issued cards also increased by 20.5%. Again, criminals are using social engineering to access bank client card data. It cannot be emphasized enough that bank clients intentionally adopt sound practices and embed them into their consciousness to protect themselves when transacting with a physical bank card or when sharing bank card details.

Digital Banking Fraud

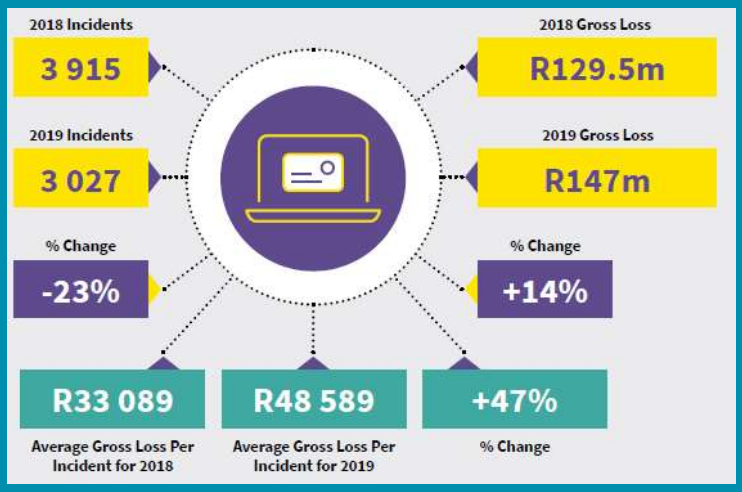


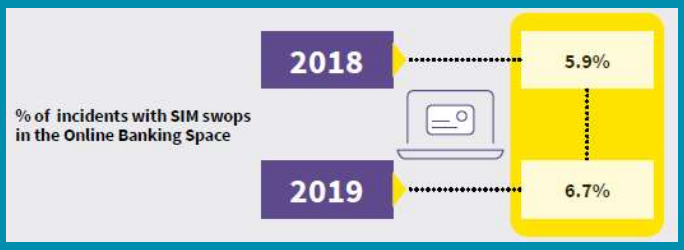


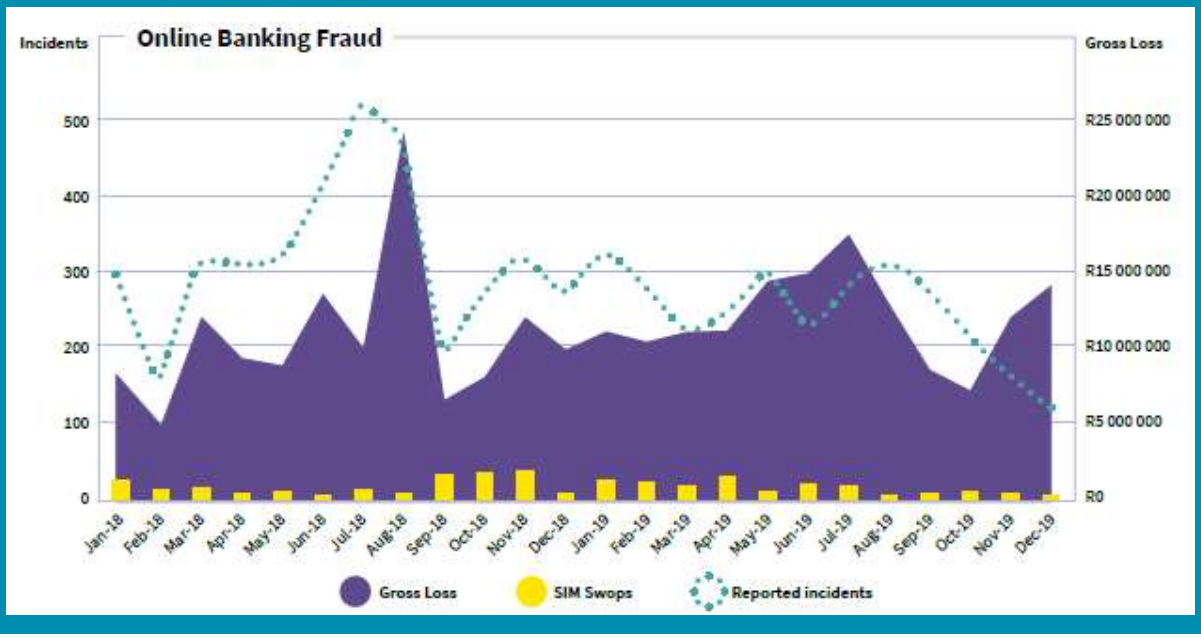




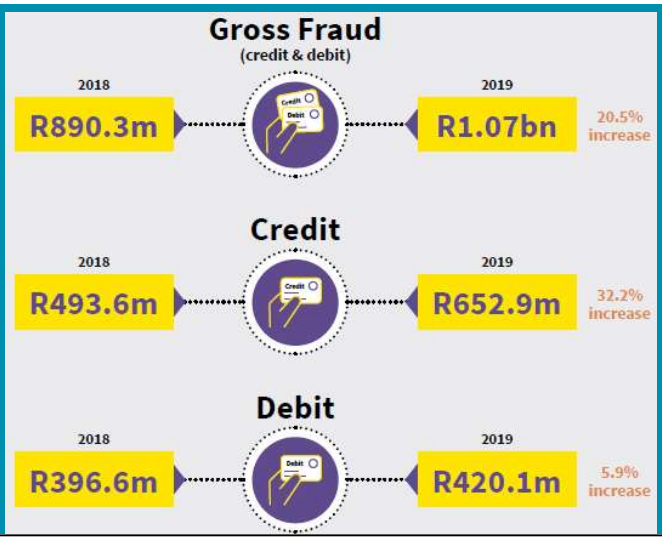
Online Banking







Debit & Credit Card Fraud Losses: All Fraud Types, All Countries



Fraud Prevention Advice

Accounting Fraud – "On the book Fraud

Fraud"

- An intentional act involving the use of deception that results in a material misstatement of financial statements.
- 'Fraud' commonly includes activities such as theft, corruption, conspiracy, On the book Fraud, money laundering, bribery, and extortion.

On the book Fraud is:

- Most common type of on the book Fraud is the misappropriation of the practice's cash and checks.

While there are approximately 41 different types of fraud, these are six that can cause the most damage.

- Financial statement fraud
- Asset misappropriation fraud
- Theft / fraud involving intellectual property and trade secrets
- Healthcare, insurance, and banking fraud
- Consumer fraud
- Cyber Fraud

Corruption

- Corrupt offenders use their influence in business transactions in a way that violates their duty of loyalty, trust and care to their employers to obtain an undue benefit for themselves or someone else.
- Bribery, extortion, and a conflict of interest.

Asset Misappropriation

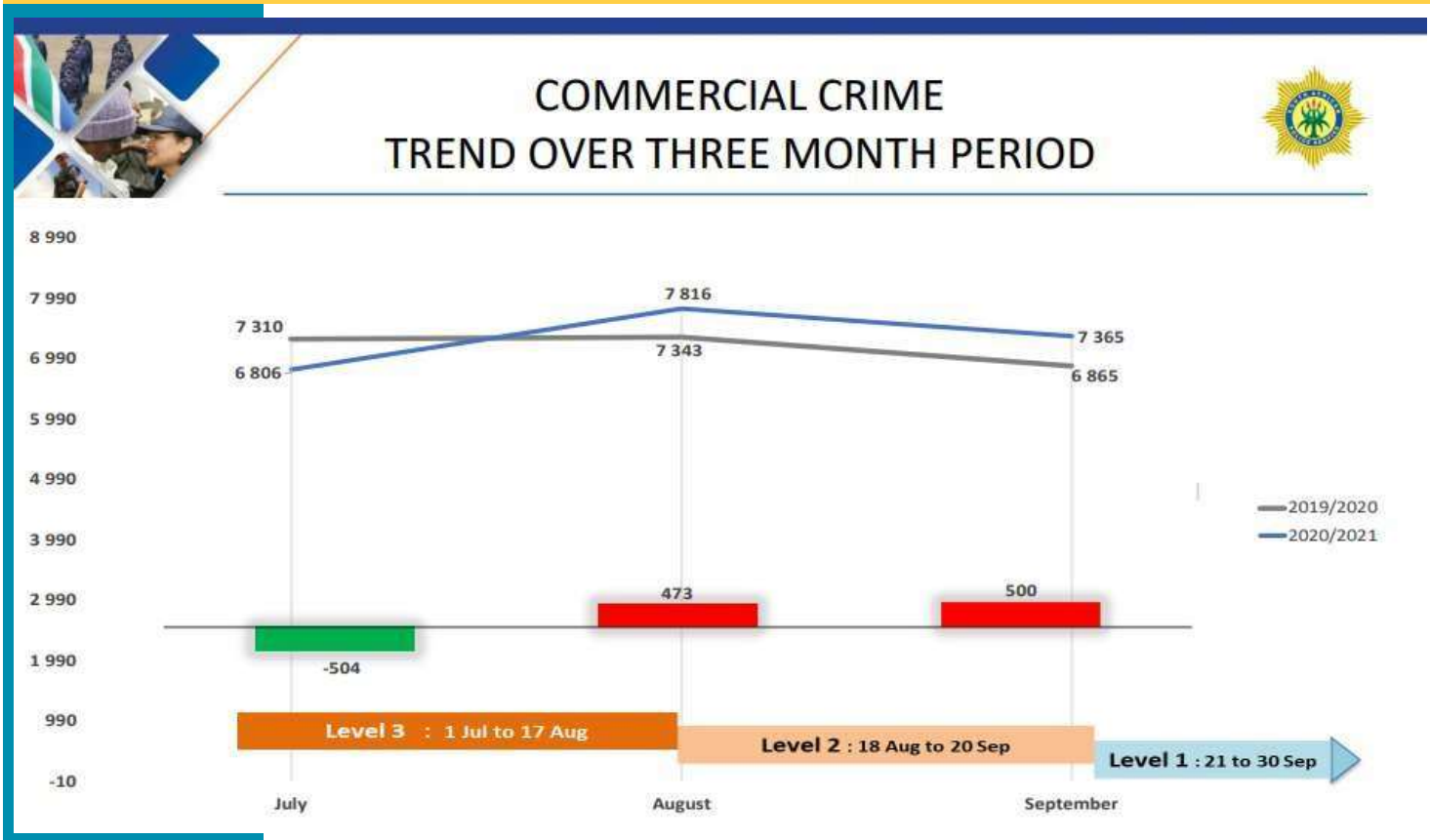
- Asset misappropriation schemes are frauds in which the perpetrator steals or misuses an organization's resources.
- An examples of asset misappropriation include a staff using a company fuel and vehicle to a private need.

Financial Statement Fraud

- Financial statement fraud involves the intentional misstatement or omission of material information from the organisation's financial re.
- *Modes Operandi*:
    - Falsification or alteration of accounting records or supporting documents
    - Misrepresentation or omission of events or transactions
    - Misapplication of accounting principle

SAPS INFORMATION BASED ON OVER THE PERIOD JULY TO SEPTEMBER 2020

Based on the SAPS crime trends for the period July 2020 to September 2020, the following statistics were published



	Eastern Cape	Free State	Gauteng	Kwazulu /Natal	Limpopo	Mpumalanga	North West	Northern Cape	Western Cape	Republic of South Africa
Jul_Sep 2019_20	2 089	1 250	7 361	3 571	1 054	1 327	1 058	301	3 507	21 518
July_Sep 2020_21	2 252	1 043	7 569	3 656	1 150	1 255	1 306	313	3 443	21 987
Case Diff	163	-207	208	85	96	-72	248	12	-64	469
%Change	7,8%	-16,6%	2,8%	2,4%	9,1%	-5,4%	23,4%	4,0%	-1,8%	2,2%

Fraud Prevention Service Offerings Available in the Market

Our team, together with strategic partners in the forensic fields, ensures a comprehensive and effective solution for our clients. Our services include, amongst others, the detection, prevention and investigation of broad-spectrum fraud, theft, and other economic offences. We specialize in fraud and theft investigations and the detection and prevention thereof. Through the collaboration with our strategic partners, we can deliver a comprehensive end-to-end service, from initial investigation stage through to judicial stage.

Proactive Services:

Assessments Due Diligence in respect of mergers and acquisitions as well as their business principals

- Work reference analysis, including:
    - Work History within a specific company are clarified to identify gaps as well as to establish any embellishments on a CV
    - Performance in all the positions held are analyzed
    - Competencies needed to be successful in future positions
    - Ethical behavior/integrity within the work environment
    - Management Concerns
    - Positions held as well as key responsibilities are clarified
    - Reason for resignation is clarified
    - Strengths and weaknesses
- Structured personal interviews
- Psychometric testing
- Verifications included in the assessment process
- Criminal record analysis
- Credit record analysis Due Diligence reviews
- Qualifications verification
- ID numbers verification
- Optional verifications:
    - Driver's license
    - Passport, citizenship, work/residence permit Records
    - FSB search for personnel in the investment environment
    - Media Search.
- Due Diligence reviews This adds value to high-level appointments where poor publicity can be to the detriment of an organization.

Reactive Services

- Criminal, civil, and disciplinary investigations
- Forensic Expert Examiners of question documents
- Corporate Governance Reviews
- Design and Implementation of Fraud Prevention Strategies
- Risk Management and Assessment
- Policy, Process and Procedure Reviews
- Regulatory Compliance
- Forensic Audits
- Due Diligence
- Fraud and corruption investigations
- Insolvency investigations
- Liaison with the SAPS for the facilitation of criminal investigations
- Liaison with the National Prosecuting Authority (NPA)
- Liaison with the Asset Forfeiture Unit of the NPA
- Investigations pertaining to the Companies Act and other legislation
- Investigations pertaining to the combating of corrupt activities as specified in legislation
- Electronic data location and deleted data recovery
- Asset location and recovery
- Insurance claim authentication investigations
- Accident reconstruction
- Labor Relations and Workplace Law Processes, including disciplinary inquiries and hearings.

RMG FORENSIC SERVICES (Pty) Ltd.

CELEBRATING 10 YEARS OF EXCELLENT SERVICE

INSTITUTE OF DIRECTORS SOUTHERN AFRICA

UNASHAMEDLYETHICAL

Introduction to Business Partner Risk Management Web-based platform

We can help you ensure business balance and ethical corporate governance through effective Business Partner Risk Management

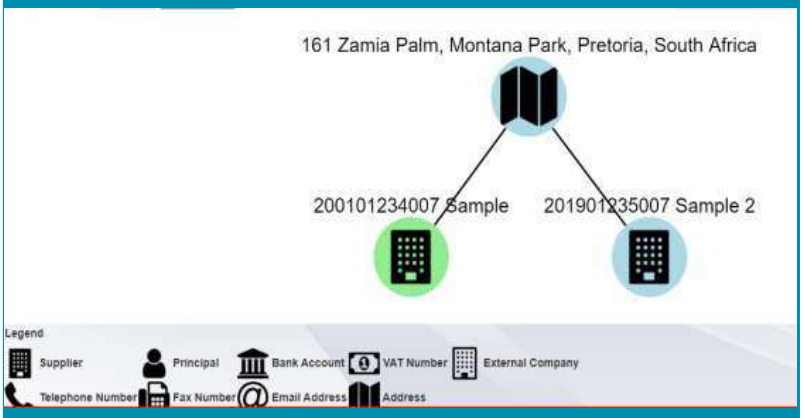
Think about the following questions:

What is the impact:

- Time it takes to update supplier documentation?
- Cost of resource allocation and time spent on the phone?
- Do you have proper processes in place ensuring you are dealing with compliant suppliers?
- Do you feel confident that your company would receive a clean compliance audit today?
- What would the impact on the business be if there is a negative outcome on the audit?
  - Fines
  - Fraud
  - Reputational damage
  - Shareholder confidence

Why Comply and why only deal with Compliant suppliers?

- Journey to sustainable **GROWTH**
- Effective way to **MANAGE** your business
- **REPUTATION** is on the line
- Competitive **EDGE**
- Result of **CUSTOMER** retention & satisfaction
- It's your **LAWFUL RESPONSIBILITY**
- **YOU** are held **LAWFUL RESPONSIBILITY** if you deal with non-compliant suppliers



RMG FORENSIC SERVICES (Pty) Ltd.

CELEBRATING 10 YEARS OF EXCELLENT SERVICE

INSTITUTE OF DIRECTORS SOUTHERN AFRICA

UNASHAMEDLYETHICAL

The following excerpt is from the South African Companies Act regarding the duties and liabilities of directors:

Directors' duties Prior to the introduction of the Act, the duties of company directors were governed by South African common law.

This dictates that **directors act in the utmost good faith** and in the best interests of their companies and includes the need to exercise care, skill, and diligence so as to promote company success through independent judgment.

Failure to properly perform the common law duties may render a director personally liable to pay monetary damages.
The Act now codifies the common law position and makes a few notable additions (which do not alter the common law position significantly).

The Act extends the duties of directors and increases the accountability of directors to the shareholders of the company.
Section 76 of the Act addresses the standard of conduct expected from directors and extends it beyond the common law duty of directors by compelling them to act honestly, in good faith and in a manner, they reasonably believe to be in the best interests of, and for the benefit of, their companies.

Section 76(3) of the Act states that a director of a company, when acting in that capacity, must exercise the powers and perform the functions of a director: in good faith and for a proper purpose; in the best interests of the company; and with the degree of care, skill and diligence that may reasonably be expected of a person carrying out the same functions in relation to the company as carried out by that director, and having the general knowledge, skill and experience of that director.

Section 76(4) of the Act states that in respect of any matter arising in the exercise of the powers or the performance of the functions of a director, a director will have satisfied the obligations in section 76(3) of the Act, if the director: has taken reasonably diligent steps to become informed about the matter; has made a decision, or supported the decision of a committee or the board with regard to that matter; and had a rational basis for believing, and did believe, that the decision was in the best interests of the company. In further compliance with this section, the director is required to communicate to the board, at the earliest practicable opportunity, any material information that comes to his or her attention, unless he or she: reasonably believes that the information is publicly available or known to the other directors; or is bound by a legal or ethical obligation of confidentiality.

Section 72 of the Act entitles companies to appoint board committees and delegate to any committee any authority of the board. Such committees may include people who are not directors of the company, but they may not be ineligible or disqualified to be a company director and may not vote on any matter to be decided by the committee.

Board committees have the full authority of the board in respect of matters referred to them and may consult with or receive advice from any person. However, the creation of any committee and the delegation of any power do not by themselves satisfy or constitute compliance by a director with his or her duties as a director.